REMARKS/ARGUMENTS

Allowable Subject Matter

The Examiner is thanked for the indication of allowable subject mater in terms of claims 5-10, 19-24, 29, 32-34.

Rejection under 35 USC § 112, first paragraph

The Examiner asserts that amendment made to claim 1 to state that the decryption key is "distinction from the encryption key string" is does not have a fair basis in the original description. With all due respect, the Applicant disagrees with this assertion.

For one thing, the whole description is about Identifier Based Encryption which inherently requires the decryption key to be distinct from the encryption key string. The original point of IBE was to encrypt data with a public identifier of the intended recipient and then have a trusted party provide the corresponding decryption key after confirming that the party requesting the decryption key was the intended recipient. If the decryption key was the same as the encryption key (a public identifier) there would be no point in doing the encryption. A brief overview of IBE is given in the description from page 1, line 29 to page 3, line 7; in particular, page 2, lines 3 to 5 state:

> "decryption key computed by the trusted authority 12 in dependence on the encryption key string and its own private data."

If the decryption key were the same as the encryption key string, there would be no need for the trusted authority to compute it.

A positive way of stating this relationship is found in the following passage starting at line 20 on page 10 of the present application:

"A public/private key pair is defined for the trusted authority 60 where the public key R is: $R \in G_1$ and the private key s is: $s \in Fq$ with $R=sP \in G_1$.

Additionally, this embodiment uses an identifier based public key Q_{ID} / private key S_{ID} pair where the Q_{ID}, $S_{ID} \in G_1$ and the trusted authority's public/private key pair (R,s) is linked with the identifier based public/private key by

$$S_{ID} = sQ_{ID} \text{ and } Q_{ID} = \text{MapToPoint } (H_1 (\text{ID}))$$

where ID is an identifier string (encryption key string)."

From this it follows:

- The identifier based key pair has a public key Q_{ID} = MapToPoint (H_1 (ID)) where ID is an identifier string (encryption key string).
- The identifier based key pair has a private key S_{ID} = sQID where s is a private key of the trusted party 60.

Clearly S_{ID} is different from Q_{ID} and from ID, the encryption key string. Lines 4-20 on page 11 describe the encryption process using Q_{ID} (renamed Q_{print}). Lines 1-10 on page 12 describe the decryption process using S_{ID} (renamed S_{print}).

This clearly shows that the encryption key string ID is distinct from the decryption key Q_{ID} (Q_{print}). So the specification teaches more than that required to support the claim amendments.

The rejection under 35 USC § 112, first paragraph, is, with all due respect, without merit and the Applicant therefore respectfully requests that this rejection be withdrawn.

Claim rejections based on the prior art

The Examiner rejects claims 1-4, 11-18, 25-28, 30, 31 and 35-38 as allegedly being fully anticipated by Peinado (US Patent Pub 2002/0013772. This grounds for rejection is respectfully traversed.

Peinado has previously been discussed by the Applicant. Please see the response dated October 10, 2007. Turning to the claims ...

Claim 1, as examined, included[1] the passage:

> "a first computing entity arranged to encrypt a first data set, the encryption done by the first computing entity being based on encryption parameters that comprise:
>
> public data of a trusted party, and
>
> an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium,"

Now, it is clear from the present Official Action (see, for example, page 2) that the examiner maps Pienado to claim 1 as follows:

Claim 1	Pienado
First data set	content
Encryption key string	content key KD
Trusted Party Public data	portable-device public key PU-BB-PD

The Pienado embodiment concerned is that described in paragraph [0271] onwards with reference to Figure 13 in which content is downloaded to a portable device that has its own black box with a respective public/private key pair PU-BB-PD / PR-BB-PD. The attached diagram on page 22 of this response summarizes what is going on.

---

[1] As is explained towards the end of this response, this passage has been amended slightly, not in a effort to change its meaning, but rather in an effort to make the antecedent terms align better within the passage.

This mapping is reasonable so far as the nature of each element is concerned. However, the Pienado public key PU-BB-PD is used to encrypt the content key KD and not as an encryption parameter for encrypting the first data set (Pienado's 'content') as is required by claim 1.

In fact, Pienado fails to anticipate claim 1 for three reasons:

- As explained above, Pienado does not encrypt a 'first data set' (Pienado's 'content'):

  "based on encryption parameters that comprise:
  public data of a trusted party, and
  an encryption key string...."

  as is required by claim 1 but only based on the key KD.

- Although in Pienado both the content key KD and the public key PU-BB-PD are used for encryption, they are not used by the same entity (KD is used by the content server and PU-BB-PD by the DRM of the user's computing device); in contrast, in claim 1, the encryption key string and trusted-party public data are used for encryption by the first computing entity (note the claim language quoted above).

- The decryption key of Pienado is the same as the encryption key (i.e. the content KD which the Examiner equates to the encryption key string of claim 1); claim 1 clearly states that the decryption key is distinct from the encryption key string.

Claim 15 includes a similar limitation, namely:

"(a) encrypting a first data set, said encrypting being based on encryption parameters that comprise:
i. public data of a trusted party, and
ii. an encryption key string comprising ..."

Claim 15 also recites "providing the output device with a decryption key, distinct from the encryption key string ...".

These limitations clearly differentiate claim 15 from the cited reference.

Claim 28, as examined, also included a similar limitation[2], namely:

"first computing entity arranged to encrypt a first data set, the encrypting done by the first computing entity being based on encryption parameters that comprise:

i. public data of a trusted party, and

ii. an encryption key string comprising …"

And claim 28 also recites "decryption key, distinct from the encryption key string, …".

These limitations clearly differentiate claim 28 from the cited reference.

Since the cited reference does not meet each and every limitation of the rejected independent claims, those rejections under 35 USC § 102 are improper and should be withdrawn.

Claim Amendments

Claims 1 and 28 have been amended slightly. The intent of these amendments is not to change the scope of these claims, but rather to make the use of antecedent terms more consistent with the amended passage.

[2] As is explained elsewhere on this page, this passage has been amended slightly, not in a effort to change its meaning, but rather in an effort to make the antecedent terms align better within the passage.

Reconsideration of the rejections and allowance of the claims are respectfully requested.

I hereby certify that this correspondence is being filed electronically with the Patent and Trademark Office, Commissioner for Patents, on

October 2, 2008
(Date of Transmission)

Stacey Dawson
(Name of Person Transmitting)

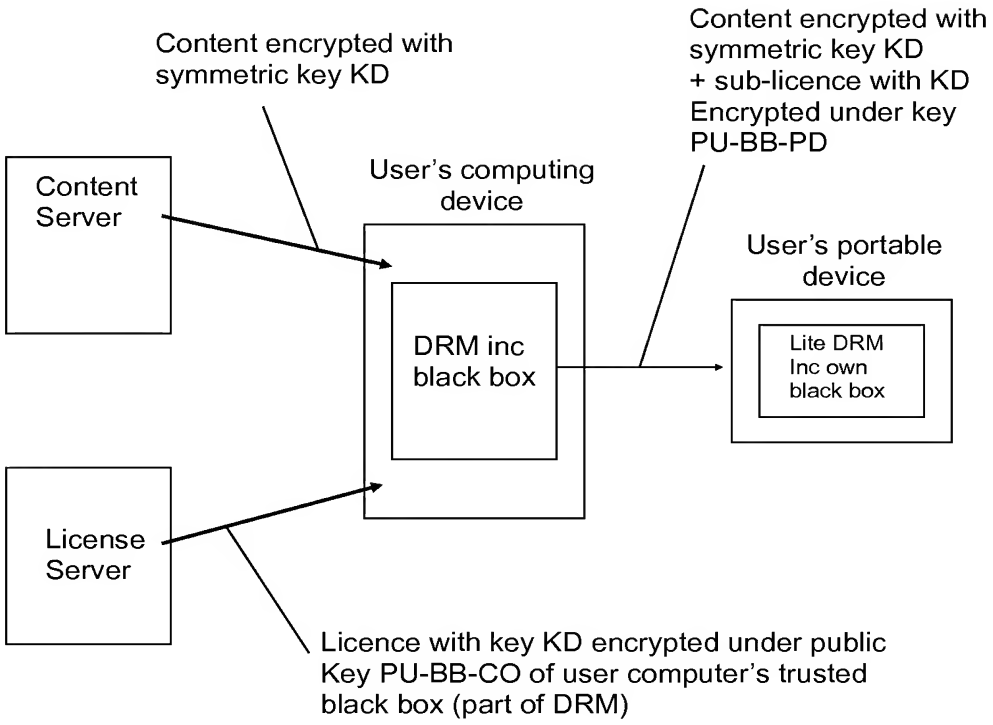
/Stacey Dawson/
(Signature)

October 2, 2008
(Date)

Respectfully submitted,

/Richard P. Berg 28145/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile


Content encrypted with symmetric key KD
Content encrypted with symmetric key KD + sub-licence with KD Encrypted under key PU-BB-PD
Content Server
User's computing device
User's portable device
DRM inc black box
Lite DRM Inc own black box
License Server
Licence with key KD encrypted under public Key PU-BB-CO of user computer's trusted black box (part of DRM)